CxP Software and Autonomy Technology Needs

Ron Morillo
SAVIO Software
ronald.morillo@jpl.nasa.gov
(818) 354-6888

CONSTELLATION

Software technology drivers

- **The Constellation Program is interested in software technologies that support the following program objectives:**
  - Build safer software-intensive systems
    - Mitigate common cause failures
  - Reduce development and schedule risk
    - Manage the size and complexity of software interactions in all phases of the life-cycle.
  - Improve fault detection, isolation and recovery techniques
  - Lower operational and maintenance cost.
  - Enable the move to greater on-board autonomy
    - Intelligent human-in-the-loop automation
  - Improve system performance analysis.
    - Timing, trending, forecasting

Specific SW technologies of interest - 1

- **Requirement Maturation:**
  - Ontology systems to determine precise meaning of requirements, avoid possible (mis) interpretations and ensure completeness of the requirement set.
  - Requirement analysis for inconsistencies and contradictions
    - Many software-related mishaps, including common cause failures, trace back to incomplete or missing requirements.

- **Design/Architecture:**
  - Capture the design knowledge once; use it to code, test and verify, operate the system.
  - Physical and behavioral models that capture system properties, cause/effects, environment and interactions:
    - Improve model-based analysis and verification, testability and timing analysis.
      - Quantify the complexity of SW code and interfaces
  - Investigate the true bounds of dissimilar software design.
  - SW fault containment concepts.

Specific SW technologies of interest - 2

- **Autonomy and FDIR:**
  - Adjustable levels of autonomy and FDIR.
  - Technology for onboard Decision Support and Expert-guided troubleshooting to crew/ Ground.
  - Tie diagnostic/prognostic tools to on-board reconfiguration managers and/or intelligent controllers.
  - Within tight timing constraints:
    - Minimize false alarms, diagnosis ambiguity.
    - Detect trends.
    - Assess failure severity for C&W.
  - Better forecasting capability (of system degradation, of remaining useful life, of impending failure..).
  - Re-planning following a failure:
    - Decompose high-level objectives onboard, incorporate locally determined information (situational awareness) and create an new execution plan.
  - When autonomy meets imperfect information: inductive reasoning techniques for managing certain degree of data inconsistency, limited knowledge or uncertain symptoms; models that manage imprecision and uncertainties.

Specific SW technologies of interest - 3

- **SW implementation:**
  - Code analyzers and compliance rule checkers.
  - Auto coding of critical software functions.

- **SW Verification and Validation:**
  - Targeting specific tests towards mitigating specific classes or types of software defects.
  - Error injection, tracing and analysis technology.
  - Model-based analysis for validation of safety-critical software designs.
  - Test suite generation, including behavioral coverage of safety-critical software functions.
  - Advanced Validation Testing that determines failure boundaries and margins for safety-critical functions.
  - Auto code tools for state estimation, data analysis and to streamline the test activity.
  - Verification and validation of autonomy and automation functions implemented in flight computers.

Specific SW technologies of interest - 4

- **Software reliability**
  - Quantifying the software risk contribution to the total risk in a system.
  - Modeling software failures.
  - Mature the technology of predictive SW/system reliability models by validating these models with operational data.